Cisco SA 500 Series Security Appliances

An All-in-One Security Solution to Secure Your Small Business

The Cisco® SA 500 Series Security Appliances, part of the Cisco Small Business Pro Series, are comprehensive gateway security solutions that combine firewall, VPN, and optional intrusion prevention and web and email security capabilities, helping you feel confident that your business is protected and resilient. These easy-to-use security appliances let you control access to network resources, enabling you to protect business data and maximize network uptime. The Cisco SA 500 Series also helps increase employee productivity by controlling web access, spam emails, phishing attacks, unauthorized intrusions, and other emerging threats, as well as by freeing IT resources from virus eradication and system cleanup activities. With the Cisco SA 500 Series, you can safely deploy new business applications without opening up security holes. Mobile employees and business partners can also securely connect to your network over the Internet using IP Security (IPsec) or Secure Sockets Layer (SSL) VPN services. With a Cisco SA 500 Series solution protecting your network, you can focus on growing your business without worrying about the latest security threats.

Challenge

The Internet has become a critical business tool for organizations of all sizes, offering new opportunities for business growth and allowing partners and remote workers to access the business network via VPN connections. But it is also a conduit for threats to enter a company's network, and these threats can have a significant negative impact:

- Unauthorized access can lead to loss of company data, unplanned downtime, and related liability concerns.
- Viruses can infect systems, bringing them down and resulting in outages and lost revenue.
- Spam and phishing create a nuisance and contribute to a loss of employee productivity.
- Spyware provides a direct inside view of your network and data that can lead to identity theft and business data loss.
- Browsing of non-work-related and harmful websites leads to lost productivity, exposure to viruses and spyware, and possible legal issues involving employees.

Solution

The Cisco SA 500 Series provides small companies with comprehensive gateway security and VPN connectivity. With its combined firewall, email, and web security capabilities, the Cisco SA 500 Series stops threats before they enter the network and affect business operations. The Cisco SA 500 Series:

- **Allows valid business traffic to flow while keeping out unwelcome visitors.** It also supports a public accessable network area, known as a demilitarized zone (DMZ), to safely host file, web, and other Internet-accessible servers without exposing the business's internal LAN network to threats.
- **Proactively prevents intrusions and blocks dangerous peer-to-peer communications:** With the optional Intrusion Prevention System (IPS) for SA 500 license, the SA 500 Series is able to identify possible intrusions into the business network and take action to stop the intrusion and prevent further risk. Additionally, the SA 500 Series can block peer-to-peer and instant messaging traffic and perform protocol inspection to help increase network security, enhance employee productivity, and keep the network available for business traffic.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- **Provides full-strength email and web protection at full speed:** With robust content security capabilities delivered via the optional Cisco ProtectLink Gateway subscription offering, the Cisco SA 500 Series provides critical perimeter security services for comprehensive protection:
  - **Full-strength protection at full speed:** ProtectLink Gateway services are delivered via a unique cloud-based approach. Emails destined for your small business are first inspected by Cisco's technology partner, Trend Micro, using enterprise-class inspection capabilities to stop a greater range of threats. For example, ProtectLink Gateway will scan your emails for more than 3 million different virus patterns and more than 400,000 spyware patterns. Additional antispam technology is provided via 10 different inspection technologies that evaluate not just the sender's network address reputation, but also the actual content of the email itself. Other small business products cannot make similar claims. In addition to the security benefits this approach provides, it avoids the compromise many other vendors make of having to slow down the bandwidth of traffic in order to inspect email and web content. With ProtectLink Gateway, more threats are stopped before they get to your business, without affecting bandwidth.
  - **Antivirus:** Award-winning antivirus technology shields your internal network resources from both known and unknown virus attacks, at the most effective point in your infrastructure, the Internet gateway. Filtering your email and web traffic at the perimeter eliminates the need for resource-intensive cleanup of an infection and helps ensure business continuity.
  - **Antispyware:** Blocking spyware at the gateway prevents it from entering your network through Internet traffic (HTTP and FTP) and email, avoiding costly spyware removal procedures and improving employee productivity.
  - **Antispam:** Effective blocking of spam, with very low false positives, helps restore the effectiveness of email, so that communication with customers, vendors, and partners continues uninterrupted.
  - **Antiphishing:** Identity theft protection guards against phishing attacks, thereby preventing employees from inadvertently disclosing company or personal details that could lead to financial loss.
  - **URL filtering:** Web and URL filtering can be used to control employee Internet usage by blocking access to inappropriate or non-work-related websites, improving employee productivity and limiting the risk of legal action by employees exposed to offensive web content.
- **Increases the security of remote access:** With support for VeriSign Indentity Protection (VIP) Services, the Cisco SA 500 Series provides two-factor authentication and one-time-use password access control for an increased level of remote access security without the need to purchase any additional authentication equipment.
- **Offers easy deployment and management:** The Cisco SA 500 Series can be managed via the embedded Security Appliance Configuration Utility, a powerful yet easy-to-use browser-based management and monitoring interface. This single solution provides comprehensive configuration and monitoring of all the services in a single application. The Security Appliance Configuration Utility can also be launched from Cisco Configuration Assistant. In addition, the Cisco SA 500 Series supports Simple Network Management Protocol (SNMP) monitoring.

Figures 1 and 2 show the interfaces for Cisco Configuration Assistant and the Security Appliance Configuration Utility.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 1. Cisco Configuration Assistant Interface

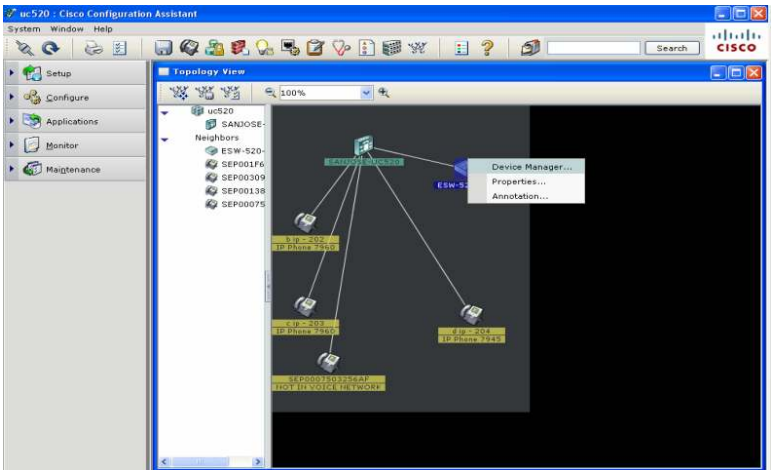

Figure 2. Security Appliance Configuration Utility Interface

Business Benefits

The Cisco SA 500 Series Security Appliances provide security and connectivity that help you:

- **Support evolving business needs:** Safely deploy new applications by providing advanced application-layer security services for a wide range of popular applications, including web-based applications, email, voice over IP (VoIP), video, and multimedia applications.
- **Enhance authentication security for remote users:** Prevent unauthorized access to your business network by using hardware- or software-generated one-time-use passwords.
- **Increase employee productivity:** Prevent the loss of employee productivity by preventing spam, spyware, and inappropriate web browsing using the Cisco ProtectLink Gateway optional service.
- **Improve business resiliency:** Prevent disruption of business-critical applications and services due to security breaches by implementing a robust business-grade firewall along with support for email and web security.
- **Reduce IT costs:** Free up IT support resources and avoid the costly process of cleaning up infections due to spyware, viruses, and other malware by preventing them from occurring.
- **Enable easy-to-deploy remote access:** Allow employees and partners to quickly and easily connect to the business with SSL VPN.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- **Achieve operational efficiency:** Reduce costs associated with deployment and ongoing management and monitoring of the security solution by using a single easy-to-install, easy-to-use solution.
- **Decrease liability:** Reduce the company's exposure to liability related to compromised data or inadequate corporate controls by implementing comprehensive access control and threat protection services in a single device.
- **Enjoy peace of mind:** Get maximum value from your Cisco solution through an affordable, subscription-based service offering. The Cisco Small Business Pro Service provides software upgrades and updates, extended access to the Cisco Small Business Support Center, and next-business-day hardware replacement.

These benefits make the Cisco SA 500 Series Security Appliance the right choice to address your security needs and enable your network and employees to deliver maximum value to your business.

Figure 3 shows the Cisco SA 500 Series Security Appliance with and without wireless connectivity.

Figure 3. Cisco SA 500 Series Security Appliances, the SA 520W and the SA 520

Product Specifications

Table 1 gives the product specifications for the Cisco SA 500 Series.

Table 1. Cisco SA 500 Series Security Appliance Models and Specifications

	SA 520	SA 520W	SA 540
Firewall			
Stateful packet inspection throughput*	200 Mbps	200 Mbps	300 Mbps
Firewall plus email and web security throughput*	200 Mbps	200 Mbps	300 Mbps
Connections	15,000	15,000	40,000
Rules	100	100	100
Schedules	Yes	Yes	Yes
IPS	Yes	Yes	Yes
Peer-to-peer and instant messaging blocking	Yes	Yes	Yes
VPN			
Triple Data Encryption Standard (3DES)/ Advanced Encryption Standard (AES) VPN throughput*	65 Mbps	65 Mbps	85 Mbps
IPsec VPN tunnels	50 max	50 max	100 max
SSL VPN tunnels	2 seats included; license required to upgrade to 25 seats (max)	2 seats included; license required to upgrade to 25 seats (max)	50 seats (max) included
Dead peer detection	Yes	Yes	Yes
IPsec Network Address Translation (NAT) traversal	Yes	Yes	Yes

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

NetBIOS broadcast over VPN	Yes	Yes	Yes
Cisco ProtectLink Gateway			
URL filtering	80+ categories	80+ categories	80+ categories
Web threat protection	Yes	Yes	Yes
Antispam protection	Yes	Yes	Yes
Virus patterns	More than 3 million	More than 3 million	More than 3 million
Spyware patterns	More than 420,000	More than 420,000	More than 420,000
Wireless			
802.11b/g/n	No	Yes	No
2 x 3 multiple input, multiple output (MIMO)	No	Yes	No
2.4 GHz	No	Yes	No
Wi-Fi Multimedia (WMM) quality of service (QoS)	No	Yes	No
Unscheduled automatic power save delivery (U-APSD) (WMM Power Save [WMM-PS])	No	Yes	No
MAC filtering	No	Yes	No
Wired Equivalent Privacy (WEP), Wi-Fi Protected Access Pre-Shared Key (WPA2-PSK), WPA2-ENT	No	Yes	No
Basic service set identifier (BSSID) or virtual access points	No	Yes; 4 supported	No
Ability to dynamically or manually adjust transmit power	No	Yes	No
Wi-Fi Protected Setup (WPS)	No	Yes	No
Other			
Routing	Static, Routing Information Protocol (RIP) v1, v2	Static, RIP v1, v2	Static, RIP v1, v2
VLANs	16	16	16
IPsec/Point-to-Point Tunneling Protocol (PPTP)/Layer 2 Tunneling Protocol (L2TP) pass-through	Yes	Yes	Yes
Message digest	MD5/SHA1/SHA2	MD5/SHA1/SHA2	MD5/SHA1/SHA2
Encryption	DES/3DES/AES	DES/3DES/AES	DES/3DES/AES
User database	100	100	400
Dynamic DNS (DDNS)	Yes	Yes	Yes
Load balancing	Yes	Yes	Yes
Integrated and automated failover and failback	Yes, using optional port for dual WAN	Yes, using optional port for dual WAN	Yes, using optional port for dual WAN
VeriSign VIP support	Yes	Yes	Yes
Physical interfaces	• All Ethernet ports 10BASE-T, 100BASE-TX, 1000BASE-T capable • 4 LAN ports • 1 WAN port • 1 optional port for use as LAN, WAN, or DMZ port • 1 USB 2.0 port • 1 power switch	• All Ethernet ports 10BASE-T, 100BASE-TX, 1000BASE-T capable • 4 LAN ports • 1 WAN port • 1 optional port for use as LAN, WAN, or DMZ port • 1 USB 2.0 port • 1 power switch • 3 external antennas	• All Ethernet ports 10BASE-T, 100BASE-TX, 1000BASE-T capable • 8 LAN ports • 1 WAN port • 1 optional port for use as LAN, WAN, or DMZ port • 1 USB 2.0 port • 1 power switch
Environmental operating temperature	32º to 104ºF (0º to 40ºC)	32º to 104ºF (0º to 40ºC)	32º to 104ºF (0º to 40ºC)
Storage temperature	–4º to 158ºF (–20º to 70ºC)	–4º to 158ºF (–20º to 70ºC)	–4º to 158ºF (–20º to 70ºC)

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Internal Power Supply			
Voltage range	90 to 264 VAC single phase	90 to 264 VAC single phase	90 to 264 VAC single phase
Input frequency	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz
Output voltage regulation	11.4V ~ 12.6V	11.4V ~ 12.6V	11.4V ~ 12.6V
Output current	Max 2.5A	Max 2.5A	Max 2.5A
Physical Specifications			
Form factor	1 RU, 19-in. rack mountable	1 RU, 19-in. rack mountable	1 RU, 19-in. rack mountable
Dimensions (H x W x D)	1.73 x 12.12 x 7.08 inches (44 x 308 x 180 mm)	1.73 x 12.12 x 7.08 inches (44 x 308 x 180 mm)without antennas	1.73 x 12.12 x 7.08 inches (44 x 308 x 180 mm)
Weight (with internal power supply)	4.91 lb (2.23 kg)	5.15 lb (2.34 kg)	5.14 lb (2.34 kg)

* Performance test methodology: Maximum performance based on RFC 2544. All results are aggregate bidirectional. Actual performance may vary depending upon network environment and configuration.

Ordering

Table 2 lists the part numbers for Cisco SA 500 Series Security Appliances.

Table 2. Product Part Numbers

Product Name	SKU
SA 520 Security Appliance	SA520-K9
SA 520W Security Appliance	SA520W-K9
SA 540 Security Appliance	SA540-K9
eDelivery Cisco ProtectLink Gateway incremental 5-seat license	L-PLGW-5=
eDelivery Cisco ProtectLink Gateway incremental 25-seat license	L-PLGW-25=
eDelivery Cisco ProtectLink Gateway incremental 5-seat license renewal	L-PLGW-5R=
eDelivery Cisco ProtectLink Gateway incremental 25-seat license renewal	L-PLGW-25R=
eDelivery IPS for SA 500 Series license	L-SA500-IPS-1YR=
eDelivery Cisco ProtectLink Endpoint incremental 5-seat license	L-PLEP-5=
eDelivery Cisco ProtectLink Endpoint incremental 25-seat license	L-PLEP-25=
eDelivery Cisco ProtectLink Endpoint incremental 5-seat license renewal	L-PLEP-5R=
eDelivery Cisco ProtectLink Endpoint incremental 25-seat license renewal	L-PLEP-25R=
eDelivery SSL license for SA 520 and SA 520W	L-FL-SSL-SA520-K9=
Cisco Small Business Pro Service, 3 years	CON-SBS-SVC2

Secure Connectivity for Your Business

The network is becoming a key part of your most important business operations. To keep your business running at its best, and to give customers the service they expect, you need a network that is secure, powerful, and flexible. The Cisco SA 500 Series Security Appliances help make communications easier by connecting customers to your business and your employees to each other. The appliances deliver the solid security, secure VPN access, and advanced routing you need. At the same time, they help you control costs, reduce your need for separate network equipment, and simplify network management. Whether you are starting up a small business or expanding a successful one, the Cisco SA 500 Series Security Appliances can help you get connected today and grow smoothly in the future.

Service and Support

The Cisco SA 500 Series Security Appliances are backed by the Cisco Small Business Pro Service, which provides affordable coverage that offers peace of mind. This subscription-based service helps you derive maximum value

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

from Cisco Small Business Pro Series products. Delivered by Cisco, this comprehensive service includes software upgrades and updates, extended access to the Cisco Small Business Support Center, and next-business-day hardware replacement as necessary. It provides community-based support to enable small businesses to share knowledge and collaborate using online forums and wikis to help boost business efficiency, identify and reduce risks, and serve customers better.

For More Information

For more information about the Cisco SA 500 Series Security Appliances, visit http://www.cisco.com/go/sa500 or contact your local Cisco provider.

For more information about the Cisco ProtectLink Gateway and Endpoint products, visit http://www.cisco.com/go/protectlink or contact your local Cisco provider.

For more information about the VeriSign VIP product, visit http://www.cisco.com/go/viptoken or contact your local Cisco provider.

For more information about the Cisco Small Business Pro Service, visit http://www.cisco.com/go/proservice.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Printed in USA C78-542899-02 11/09

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.